APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,805	02/27/2004	Michael D. Smith	418268001US	5629

45979   7590   04/19/2011
PERKINS COIE LLP/MSFT
P. O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER
STRODER, CARRIE A

ART UNIT	PAPER NUMBER
3689	

NOTIFICATION DATE	DELIVERY MODE
04/19/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentprocurement@perkinscoie.com

	Application No.	Applicant(s)
Office Action Summary	10/789,805	SMITH ET AL.
	Examiner	Art Unit	
	CARRIE A. STRODER	3689	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *15 February 2011*.

2a) ☒ This action is **FINAL**.　　　　2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1,2,5,6 and 9-22* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1, 2, 5, 6, and 9-22* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All　b) ☐ Some * c) ☐ None of:

　　　1. ☐ Certified copies of the priority documents have been received.

　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
　　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)　　　　　　　　**Office Action Summary**　　　　　　Part of Paper No./Mail Date 20110411

DETAILED ACTION

1.   This is in response to the applicant's communication filed

on 15 February 2011, wherein:

   Claims 1, 2, 5, 6, and 9-22 are currently pending;

   claims 3, 4, 7, 8, and 23-30 are cancelled; and

   claims 1 and 10 are currently amended.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs

of 35 U.S.C. 102 that form the basis for the rejections under

this section made in this Office action:

   A person shall be entitled to a patent unless –

   (e) the invention was described in (1) an application for patent, published
   under section 122(b), by another filed in the United States before the
   invention by the applicant for patent or (2) a patent granted on an
   application for patent by another filed in the United States before the
   invention by the applicant for patent, except that an international
   application filed under the treaty defined in section 351(a) shall have the
   effects for purposes of this subsection of an application filed in the
   United States only if the international application designated the United
   States and was published under Article 21(2) of such treaty in the English
   language.

2.   **Claims 1, 5-6, 10-11, 13-15, and 17-22 are rejected under**

35 U.S.C. 102(e) as being anticipated by McCorkendale et al. (US

20040153644).

Referring to claim 1:

McCorkendale teaches

when installing an application (paragraph 56; "controls the installation and/or execution"),

establishing a limit on services of a service provider that the application is authorized to use based on published requirements of the application, the service provider being a computer system that is remote to the consumer system (paragraphs 36 & 51 & Fig. 1; "allows the software developer to securely transmit an application program or other piece of software to the certifying authority as part of a request to certify the software. Moreover, the module allows the software developer to receive a certified copy of the software back from the certifying authority" where "certifying authority" is interpreted as the service provider and the request to certify the software is interpreted as the "service" and "the frequency monitoring module tracks software execution frequencies over sliding time windows. For example, the module can track the number of execution requests for a particular piece of software in any given hour. If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious...the thresholds can be set based on trust level information included with the software" where the trust level

information included with the software is interpreted as published requirements" and where the "certifying authority" in Fig. 1 is interpreted as the service provider and the "client device" is interpreted as the consumer computer);

asking the service provider if the application is authorized to use the service provider wherein the service provider determines that the application is not authorized based on notifications received from other consumer systems indicating that the application is misbehaving (paragraphs 49-50; "This module 522 is adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices");

determining by the processor whether the application is authorized to request services of the service provider based on a response to the asking of the service provider if the application is authorized to use the service provider (paragraphs 49-50; "the malicious software detection module updates the software's status in the database module to 'deny'" and "is adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices");

when it is determined that the application is authorized to request services of the service provider, installing the

application (paragraphs 57-58; "allows the installation routine
to install only approved software" and "this description uses
the term 'execute' to mean 'execute and/or install'"); and

when it is determined that the application is not
authorized to request services of the service provider, not
installing the application (paragraphs 57-58; "allows the
installation routine to install only approved software" and
"this description uses the term 'execute' to mean 'execute
and/or install'").

under control of a runtime environment after the
application has been installed (paragraph 56; "controls the
installation and/or execution"),

providing the application executing on the consumer system
with access to an indication of the established limit so that
the application can know and abide by the established limit
(paragraph 58; where stopping the installation and/or execution
of certain software is interpreted as an indication of the
established limit and where "so that the application can know
and abide by the established limit" is not a positive claim
limitation and therefore, receives little patentable weight);

when the application executing on the consumer system
requests a service of the service provider (paragraph 51 and 58;
"the module can track the number of execution requests" where

the service being provided is the granting or denial of

permission for the software to execute and "Therefore, the

present invention includes client devices 122 that perform the

gatekeeping function *during* (or prior to) installation of

software and client devices that perform the gatekeeping

function *during* (or prior to) execution of software." [emphasis

added]),

   determining by the processor whether the request would

exceed the established limit that is based on published

requirements of the application (paragraph 51; "If the number of

executions exceeds a predetermined threshold, the module

determines that the software is malicious");

   when it is determined that the request would not exceed the

established limit, requesting the service provider to provide

the service (paragraphs 46-51; "If the number of executions

exceeds a predetermined threshold, the module determines that

the software is malicious" and "If the heuristics indicate that

software is malicious, the malicious software detection module

updates the software's status in the database module to 'deny'"

and "the default status is 'allow' because the software is

certified by the certifying authority and presumably safe"); and

   when it is determined that the request would exceed the

established limit (paragraph 51; "If the number of executions

exceeds a predetermined threshold, the module determines that
the software is malicious"),

notifying the service provider that the application is
misbehaving (paragraphs 49 & 51; "If the number of executions
exceeds a predetermined threshold, the module determines that
the software is malicious" and "If the heuristics indicate that
software is malicious, the malicious software detection module
updates the software's status in the database module to 'deny'"
and where updating the software's status in the database module
is interpreted as notifying the service provider); and

prohibiting execution of the application on the consumer
system (paragraphs 46-51; "If a client device requests to
execute software marked as 'deny' in the database module, the
detection module will report this status back to the client
device, thereby preventing the software from being executed").

Referring to claim 10:

McCorkendale teaches

providing an indication of misbehavior for the application
when the application requests services of the service provider,
the service provider being a computer system that is remote to
the consumer system (paragraphs 36 & 49-51 & Fig. 1; "If the
heuristics indicate that software is malicious, the malicious

software detection module updates the software's status in the

database module to 'deny'" and "the frequency monitoring module

tracks software execution frequencies over sliding time windows.

For example, the module can track the number of execution

requests for a particular piece of software in any given hour.

If the number of executions exceeds a predetermined threshold,

the module determines that the software is malicious…the

thresholds can be set based on trust level information included

with the software" and where the "certifying authority" in Fig.

1 is interpreted as the service provider and the "client device"

is interpreted as the consumer computer);

executing by the consumer system the application (paragraph

58; "Therefore, the present invention includes client devices

122 that perform the gatekeeping function during (or prior to)

installation of software and client devices that perform the

gatekeeping function *during* (or prior to) *execution* of

software." where *during execution* requires execution of the

application by the consumer system) and

under control of a runtime environment executing on the

consumer system (paragraph 56; "A gatekeeper module 612 in the

client device 122 controls the installation and/or execution…"),

when the executing application requests a service of the

service provider (paragraphs 9 and 51; "At some point, one or

more of the client devices (122) attempts (714) to execute (as
used herein, "execute" also includes "install") the software. As
part of this process, the client device (122) determines (716)
whether the software is potentially malicious" and "the module
can track the number of execution requests" where the service
being provided is the granting or denial of permission for the
software to execute),

determining by the processor whether the application is
behaving in accordance with the indication of the misbehavior
(paragraph 51; "If the number of executions exceeds a
predetermined threshold, the module determines that the software
is malicious");

when it is determined that the application is not behaving
in accordance with the indication of misbehavior, requesting by
the runtime environment, the service provider to provide the
service (paragraphs 69; "If the client device 122 cannot
determine whether the software is potentially malicious, i.e.,
its status is "unknown," the client device 122 typically blocks
execution of the software and optionally sends 724 a copy of the
software to the analysis authority 120 for evaluation."); and

when it is determined that the application is behaving in
accordance with the indication of misbehavior (paragraph 51; "If

the number of executions exceeds a predetermined threshold, the
module determines that the software is malicious"),

notifying the service provider that the application is
misbehaving so that the service provider can determine whether
the application is misbehaving and revoke authorization of the
application to use the service provider when executing on the
consumer system or when executing on other consumer systems
(paragraphs 49 & 51; "If the number of executions exceeds a
predetermined threshold, the module determines that the software
is malicious" and "If the heuristics indicate that software is
malicious, the malicious software detection module updates the
software's status in the database module to 'deny'" and where
updating the software's status in the database module is
interpreted as notifying the service provider); and

prohibiting continued execution of the application
(paragraphs 46-51; "If a client device requests to execute
software marked as 'deny' in the database module, the detection
module will report this status back to the client device,
thereby preventing the software from being executed").

Referring to claims 5 and 14:

McCorkendale teaches wherein the service provider
aggregates notifications provided by different consumer systems

to determine whether the application should be authorized to

request services of the service provider (paragraph 50; "declare

that software is potentially malicious upon the occurrence of an

abnormally high frequency of requests from different client

devices to execute the same software within a relatively short

time period").

Referring to claims 6 and 15:

McCorkendale teaches the service provider aggregates

notifications provided by the consumer system to determine

whether the consumer system should not be authorized to request

services of the service provider (paragraph 50; "that detects

potentially malicious software based on the frequency of

software execution requests received from the client devices").

Referring to claim 11:

McCorkendale teaches wherein the indication of misbehavior

is exceeding a number of requests for services of the service

provider (paragraph 51; "If the number of executions exceeds a

predetermined threshold, the module determines that the software

is malicious").

Referring to claim 13:

McCorkendale teaches before installing the application
determining whether the application is authorized to request
services of the service provider (paragraph 56; "software cannot
be installed and/or executed without permission from it").

Referring to claim 17:

McCorkendale teaches

when service consumers determine that the application is
misbehaving, receiving by the service provider notifications of
the misbehavior from the service consumers, wherein the
application misbehaves when the application requests certain
services of the service provider, each service consumer being a
consumer computer that is different from the computer system of
the service provider (paragraphs 58-59; "Therefore, the present
invention includes client devices 122 that perform the
gatekeeping function during (or prior to) installation of
software and client devices that perform the gatekeeping
function during (or prior to) execution of software. In a
similar manner, the frequency monitoring module 522 in the
execution authority 118 can utilize installation and/or
execution frequency statistics to detect malicious software.");

determining by the processor whether a condition of
misbehavior is satisfied based on the received notifications
from different consumers indicating that the application is
misbehaving when executed by the different consumers (paragraphs
49-50; "the malicious software detection module updates the
software's status in the database module to 'deny'" and "is
adapted to declare that software is potentially malicious upon
the occurrence of an abnormally high frequency of requests from
different client devices"); and

when a service request is received to provide services to
the application and it is determined that the condition of
misbehavior is satisfied, refusing to provide the requested
service (paragraphs 46-51; "If the number of executions exceeds
a predetermined threshold, the module determines that the
software is malicious" and "If a client device requests to
execute software marked as 'deny' in the database module, the
detection module will report this status back to the client
device, thereby preventing the software from being executed").

Referring to claim 18:

McCorkendale teaches wherein the condition of misbehavior
is when multiple service consumers provide notifications that
the application has attempted to exceed an established limit of

requests for services from the service provider (paragraph 50;

"adapted to declare that software is potentially malicious upon

the occurrence of an abnormally high frequency of requests from

different client devices").

Referring to claim 19:

McCorkendale teaches receiving from another service

provider a notification that the application is misbehaving

wherein the condition of misbehavior is satisfied based on the

notification received from another service provider (paragraph

32; "the execution authority notifies the analysis authority

when the execution authority detects a possible software worm"

and where the execution and analysis authorities are interpreted

as service providers).

Referring to claim 20:

McCorkendale teaches notifying service consumers that the

application is not authorized to request services of the service

provider (paragraph 52; "this module sends 'malicious software'

alerts to the client devices").

Referring to claim 21:

McCorkendale teaches wherein a service consumer requests
the service provider to indicate whether the application is
authorized (paragraph 36; "this module allows the software
developer to securely transmit an application program or other
piece of software to the certifying authority as part of a
request to certify the software" and where the software
developer is interpreted as a service consumer and the
certifying authority is interpreted as the service provider).

Referring to claims 22:

McCorkendale teaches wherein the condition of misbehavior
is based on an aggregation of the service consumer notifications
(paragraph 50; "declare that software is potentially malicious
upon the occurrence of an abnormally high frequency of requests
from different client devices to execute the same software
within a relatively short time period").

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which
forms the basis for all obviousness rejections set forth in this
Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

2.   The factual inquiries set forth in *Graham* **v.** *John Deere*

Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for

establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

    1.   Determining the scope and contents of the prior art.
    2.   Ascertaining the differences between the prior art and
          the claims at issue.
    3.   Resolving the level of ordinary skill in the pertinent
          art.
    4.   Considering objective evidence present in the
          application indicating obviousness or nonobviousness.

1.   **Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as**

being unpatentable over McCorkendale et al. (US 20040153644) as

applied to claims 1 and 10 above, in view of Davis et al. (US

20030135509).

    Referring to claims 2 and 12:

    McCorkendale does not disclose wherein the prohibiting

includes uninstalling the application. However, Davis discloses

wherein the prohibiting includes uninstalling the application

(paragraph 64).

It would have been obvious to one of ordinary skill in the
art at the time of applicant's invention to modify the teaching
of McCorkendale by uninstalling the application as taught by
Davis because this would provide a way to completely remove an
application that was misbehaving, thereby preventing a possible
virus.

2.   **Claim 9 is rejected under 35 U.S.C. 103(a) as being
unpatentable over McCorkendale et al. (US 20040153644) as
applied to claim 1, above, in view of Choate (US 20010054026).**

Referring to claim 9:

McCorkendale does not teach wherein multiple service
providers can provide equivalent services and the application
can requests services one of those service providers as
designated by the consumer system. However, Choate teaches
wherein multiple service providers can provide equivalent
services and the application can requests services one of those
service providers as designated by the consumer system
(paragraph 26).

It would have been obvious to one of ordinary skill in the
art at the time of applicant's invention to modify the teaching
of McCorkendale as taught by Choate because this would provide

the ability to continue to provide services to customers while
the system is fixed.

3.   **Claim 16 is rejected under 35 U.S.C. 103(a) as being
unpatentable over McCorkendale et al. (US 20040153644) as
applied to claim 10, above, in view of Choate (US 20010054026).**

     Referring to claim 16:

     Liang does not teach wherein the limit is established by a
user of a consumer system. However, Choate teaches wherein the
limit is established by a user of a consumer system (paragraph
31).

     It would have been obvious to one of ordinary skill in the
art at the time of applicant's invention to modify the teaching
of McCorkendale by allowing the user to establish a limit as
taught by Choate because the user is the one who is actually
using the services and is in the best position to determine what
is abnormal, which would provide a more accurate assessment of
whether the system is misbehaving.

Response to Arguments

Applicant's arguments filed 15 February 2011 have been
fully considered but they are not persuasive.

Applicant argues that the prior art does not teach that the
application is executing when the service is requested.
Examiner respectfully disagrees. McCorkendale states, in
paragraph 58, "...the present invention includes client devices
122 that perform the gatekeeping function...*during*...execution of
software" (emphasis added).

Contact

Any inquiry concerning this communication or earlier
communications from the examiner should be directed to CARRIE A.
STRODER whose telephone number is (571)270-7119. The examiner
can normally be reached on Monday - Thursday 8:00 a.m. - 5:00
p.m. ET.

If attempts to reach the examiner by telephone are
unsuccessful, the examiner's supervisor, Jan Mooneyham can be
reached on (571)272-6805. The fax phone number for the
organization where this application or proceeding is assigned is
571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CARRIE A. STRODER/
Examiner, Art Unit 3689
/Dennis Ruhl/
Primary Examiner, Art Unit 3689